EAST Search History

Ref #	Hits	Search Query	DBs	Default Operator	Plurals	Time Stamp
S1	2744	713/200-202.ccls.	USPAT	OR	OFF	2004/12/01 12:40
S2	138	S1 and virus with software	US-PGPUB; USPAT	OR	OFF	2004/12/01 12:41
S3	66	S2 and (date$2 hour minute time$2) with (virus infect$5)	US-PGPUB; USPAT	OR	ON	2004/12/01 12:48
S4	0	S2 and (date$2 hour minute time$2) adj of adj (virus infect$5)	US-PGPUB; USPAT	OR	ON	2004/12/01 12:48
S5	44	S2 and (date$2 hour minute time$2) near3 (virus infect$5)	US-PGPUB; USPAT	OR	ON	2004/12/01 12:48
S6	32	S2 and (date$2 hour minute time$2) near2 (virus infect$5)	US-PGPUB; USPAT	OR	ON	2004/12/01 12:55
S7	29	server$2 with virus$2 with detect$5 and @ad<="20010330"	US-PGPUB; USPAT	OR	ON	2004/12/01 13:17
S8	5	server$2 with virus$2 with detect$5 and @ad<="20010330" and (display with (virus infect$5) with (information stat$6 data))	US-PGPUB; USPAT	OR	ON	2004/12/01 13:18
S9	101	726/24.ccls.	USPAT	OR	OFF	2006/01/08 13:32
S11	1	726/24.ccls. and (communication$4 near2 (log$2 history$2 record$2)) with virus$2	US-PGPUB; USPAT; USOCR; EPO; JPO; DERWENT; IBM_TDB	OR	OFF	2006/01/08 13:33
S12	4	726/24.ccls. and (communication$4 near2 (log$2 history$2 record$2))	US-PGPUB; USPAT; USOCR; EPO; JPO; DERWENT; IBM_TDB	OR	OFF	2006/01/08 13:34
S13	12	726/24.ccls. and ((time$2 adj detect$4))	US-PGPUB; USPAT; USOCR; EPO; JPO; DERWENT; IBM_TDB	OR	OFF	2006/01/08 13:34
S14	219	726/24.ccls.	US-PGPUB; USPAT; USOCR; EPO; JPO; DERWENT; IBM_TDB	OR	OFF	2006/01/08 14:05

EAST Search History

S15	38	726/24.ccls. and (scan$4 monitor$4 log$2 watch$3) with (communication$2)	US-PGPUB; USPAT; USOCR; EPO; JPO; DERWENT; IBM_TDB	OR	OFF	2006/01/09 11:11
S16	204	726/24.ccls. and (scan$4 monitor$4 log$2 watch$3)	US-PGPUB; USPAT; USOCR; EPO; JPO; DERWENT; IBM_TDB	OR	OFF	2006/01/10 14:16
S17	9	(display$4 with time$2 with virus$2 with user$2)	US-PGPUB; USPAT; USOCR; EPO; JPO; DERWENT; IBM_TDB	OR	OFF	2006/01/10 14:19
S18	844	((show$2 notify display$4) with (hour$2 date$2 time$2) with (infection$2 virus$2)) and (computer server pc)	US-PGPUB; USPAT; USOCR; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2006/01/10 14:25
S19	17	((show$2 notif$3 display$4) with (hour$2 date$2 time$2) with (infection$2 virus$2) with (user$2)) and (computer server pc)	US-PGPUB; USPAT; USOCR; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2006/01/10 17:02
S20	8	(time with infection$2) and "713"/$. ccls. and "726"/$.ccls.	US-PGPUB; USPAT; USOCR; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2006/01/10 17:04
S21	58	(time with infection$2) and ("713"/$.ccls. or "726"/$.ccls.)	US-PGPUB; USPAT; USOCR; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2006/01/10 17:07
S22	2	(((history$2 log) with communication$2) same (time with infection$2)) and ("713"/$.ccls. or "726"/$.ccls.)	US-PGPUB; USPAT; USOCR; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2006/01/10 17:10

EAST Search History

S23	0	(report$2 with (time with infection$2)) and ("713"/$.ccls. or "726"/$.ccls.)	US-PGPUB; USPAT; USOCR; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2006/01/10 17:11
S24	21	(report$2 with ((date time) with (virus infection$2))) and ("713"/$. ccls. or "726"/$.ccls.)	US-PGPUB; USPAT; USOCR; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2006/01/10 17:20
S25	32	((display$2 show$2) with ((date time) with (virus infection$2))) and ("713"/$.ccls. or "726"/$.ccls.)	US-PGPUB; USPAT; USOCR; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2006/01/10 18:24
S26	0	intrustion adj detect$5 and conklin. in.	US-PGPUB; USPAT; USOCR; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2006/01/10 18:24
S27	1	intrusion adj detect$5 and conklin. in.	US-PGPUB; USPAT; USOCR; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2006/01/10 18:24
S28	8	continu$6 with (monitor$4 watch$4 scan$4 search$4) near3 virus$$ and ((time date) with (infect$3 detect$3)) same (display$4 show$4 send$$)	US-PGPUB; USPAT	OR	ON	2006/01/11 12:45
S29	31	continu$6 with (monitor$4 watch$4 scan$4 search$4) near3 virus$$ and ((time date) with (infect$3 detect$3))	US-PGPUB; USPAT	OR	ON	2006/01/11 16:25
S32	220	726/24.ccls.	US-PGPUB; USPAT	OR	ON	2006/01/11 16:47
S33	220	726/24.ccls.	US-PGPUB; USPAT; USOCR; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2006/01/11 16:47

EAST Search History

S34	389	726/24.ccls.	US-PGPUB; USPAT; USOCR; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2006/12/07 17:22
S35	31	726/24.ccls. and ((path route) with (infect$4 virus$2))	US-PGPUB; USPAT; USOCR; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2006/12/07 17:38
S36	389	726/24.ccls.	US-PGPUB; USPAT; USOCR; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2006/12/07 18:09
S37	2	"5991881".pn.	US-PGPUB; USPAT; USOCR; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2006/12/07 18:10
S38	42401	((time date) with (infection virus intrusion))	US-PGPUB; USPAT; USOCR; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2006/12/07 18:13
S39	1211	((time date) with (infection virus intrusion)) same ((history log$4))	US-PGPUB; USPAT; USOCR; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2006/12/07 18:13
S40	29	((time date) with (infection virus intrusion)) same ((history log$4)) same (install$4)	US-PGPUB; USPAT; USOCR; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2006/12/07 18:13
S41	35	((time date) with (infection virus intrusion)) same ((history log$4)) same (install$6)	US-PGPUB; USPAT; USOCR; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2006/12/07 18:14
S42	6518	time near2 infect$4	US-PGPUB; USPAT	OR	ON	2006/12/11 15:26

EAST Search History

S43	26	(time near2 infect$4) same (time near2 detect$4) and (virus)	US-PGPUB; USPAT	OR	ON	2006/12/11 15:27
S44	55	(time near2 infect$4) same (computer with virus)	US-PGPUB; USPAT	OR	ON	2006/12/20 16:18
S45	735	726/22.ccls.	US-PGPUB; USPAT	OR	ON	2006/12/20 16:18

S46	735	726/22.ccls.	US-PGPUB;
			USPAT;
			USOCR;
			FPRS;
			EPO; JPO;
			DERWENT;
			IBM_TDB
				OR	ON	2006/12/20 16:18

S47	486	726/23.ccls.	US-PGPUB;
			USPAT;
			USOCR;
			FPRS;
			EPO; JPO;
			DERWENT;
			IBM_TDB
				OR	ON	2006/12/20 16:18

S48	3	726/24.ccls. and (time with installation).clm.	US-PGPUB;
			USPAT;
			USOCR;
			FPRS;
			EPO; JPO;
			DERWENT;
			IBM_TDB
				OR	ON	2006/12/20 16:19

S49	519	naitoh.in.	US-PGPUB;
			USPAT;
			USOCR;
			FPRS;
			EPO; JPO;
			DERWENT;
			IBM_TDB
				OR	ON	2006/12/20 16:19

S50	4	naitoh.in. and (virus)	US-PGPUB;
			USPAT;
			USOCR;
			FPRS;
			EPO; JPO;
			DERWENT;
			IBM_TDB
				OR	ON	2006/12/20 16:20

S51	391648	fujitsu.as.	US-PGPUB;
			USPAT;
			USOCR;
			FPRS;
			EPO; JPO;
			DERWENT;
			IBM_TDB
				OR	ON	2006/12/20 16:20

EAST Search History

S52	116	fujitsu.as. and (virus infection) with (computer terminal)	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2006/12/20 16:21
S53	1	fujitsu.as. and (virus infection) with (computer terminal) and (time adj install$6).clm.	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2006/12/20 16:21

PORTAL

USPTO

Subscribe (Full Service) Register (Limited Service, Free) Login

Search: ● The ACM Digital Library ○ The Guide

virus, detection, time, installation SEARCH

THE ACM DIGITAL LIBRARY

Feedback Report a problem Satisfaction survey

Terms used **virus** **detection** **time** **installation**

Found **57,113** of **193,448**

Sort results by: relevance

Display results: expanded form

Save results to a Binder

Search Tips

□ Open results in a new window

Try an Advanced Search
Try this search in The ACM Guide

Results 1 - 20 of 200 Result page: **1** 2 3 4 5 6 7 8 9 10 next

Best 200 shown

Relevance scale □□■■■

1 Technical correspondence: Analysis and detection of computer viruses and worms: an annotated bibliography
Prabhat K. Singh, Arun Lakhotia
February 2002 **ACM SIGPLAN Notices**, Volume 37 Issue 2
Publisher: ACM Press
Full text available: pdf(667.42 KB) Additional Information: full citation, abstract

This annotated bibliography reviews research in analyzing and detecting computer viruses and worms. This document focuses on papers that give information about techniques and systems detecting malicious code.

2 Intrusion detection and response: Predators: good will mobile codes combat against computer viruses
Hiroshi Toyoizumi, Atsuhi Kara
September 2002 **Proceedings of the 2002 workshop on New security paradigms**
Publisher: ACM Press
Full text available: pdf(526.24 KB) Additional Information: full citation, abstract, references, citings, index terms

We present a mathematical analysis of a new approach to fight against computer viruses through the use of their predators. Predators are good will mobile codes which, like viruses, travel over computer networks, and replicate and multipy themselves. The only difference is that predators are specifically designed to eliminate the viruses. We model the interaction between predators and viruses by the Lotka-Volterra equations, which are widely used in mathematical biology. Using this model, we deri ...

Keywords: Lotka-Volterra equation, computer virus, mathematical biology, worms

3 A taxonomy of computer program security flaws
Carl E. Landwehr, Alan R. Bull, John P. McDermott, William S. Choi
September 1994 **ACM Computing Surveys (CSUR)**, Volume 26 Issue 3
Publisher: ACM Press
Full text available: pdf(3.81 MB) Additional Information: full citation, abstract, references, citings, index terms, review

An organized record of actual flaws can be useful to computer system designers, programmers, analysts, administrators, and users. This survey provides a taxonomy for computer program security flaws, with an Appendix that documents 50 actual security flaws. These flaws have all been described previously in the open literature, but in widely separated places. For those new to the field of computer security, they provide a good introduction to the characteristics of security flaws and how they ...

Keywords: error/defect classification, security flaw, taxonomy

4 Session 1: ACT: attachment chain tracing scheme for email virus detection and control
Jintao Xiong
October 2004 **Proceedings of the 2004 ACM workshop on Rapid malcode**
Publisher: ACM Press
Full text available: pdf(283.77 KB) Additional Information: full citation, abstract, references, index terms

Modern society is highly dependent on the smooth and safe flow of information over communication and computer networks. Computer viruses and worms pose serious threats to the society by disrupting the normal information flow and collecting or destroying information without authorization. Compared to the effectiveness and ease of spreading worms and viruses, currently adopted defense schemes are slow to react and costly to implement.

This paper proposes an automated email virus detecti ...

Keywords: contact tracing, transmission chain, worm defense

5 Risks to the public in computers and related systems
Peter G. Neumann
April 1993 **ACM SIGSOFT Software Engineering Notes**, Volume 18 Issue 2
Publisher: ACM Press
Full text available: pdf(1.60 MB) Additional Information: full citation, citings, index terms

6 Security as a new dimension in embedded system design: Security as a new dimension in embedded system design
Srivaths Ravi, Paul Kocher, Ruby Lee, Gary McGraw, Anand Raghunathan
June 2004 **Proceedings of the 41st annual conference on Design automation**
Publisher: ACM Press
Full text available: pdf(209.10 KB) Additional Information: full citation, abstract, references, citings, index terms

The growing number of instances of breaches in information security in the last few years has created a compelling case for efforts towards secure electronic systems. Embedded systems, which will be ubiquitously used to capture, store, manipulate, and access data of a sensitive nature, pose several unique and interesting security challenges. Security has been the subject of intensive research in the areas of cryptography, computing, and networking. However, despite these efforts, *security is ...*

***Keywords**: PDAs, architectures, battery life, cryptography, design, design methodologies, digital rights management, embedded systems, performance, security, security processing, security protocols, sensors, software attacks, tamper resistance, trusted computing, viruses*

7 Robust service: Rewind, repair, replay: three R's to dependability
Aaron B. Brown, David A. Patterson
July 2002 **Proceedings of the 10th workshop on ACM SIGOPS European workshop: beyond the PC EW10**
Publisher: ACM Press
Full text available: pdf(146.14 KB) Additional Information: full citation, abstract, references

Motivated by the growth of web and infrastructure services and their susceptibility to human operator-related failures, we introduce *system-level undo* as a recovery mechanism designed to improve service dependability. Undo enables system operators to recover from their inevitable mistakes and furthermore enables *retroactive repair* of problems that were not fixed quickly enough to prevent detrimental effects. We present the "three R's", a model of undo that matches the needs of huma ...

8 Defensive techniques: Proactive security for mobile messaging networks
Abhijit Bose, Kang G. Shin
September 2006 **Proceedings of the 5th ACM workshop on Wireless security WiSe '06**
Publisher: ACM Press
Full text available: pdf(281.53 KB) Additional Information: full citation, abstract, references, index terms

The interoperability of IM (Instant Messaging) and SMS (Short Messaging Service) networks allows users to seamlessly use a variety of computing devices from desktops to cellular phones and mobile handhelds. However, this increasing convergence has also attracted the attention of malicious software writers. In the past few years, the number of malicious codes that target messaging networks, primarily IM and SMS, has been increasing exponentially. Large message volume and number of users in these ...

Keywords: Instant Messaging (IM), SMS/MMS, containment, mobile viruses, proactive security, worms

9 Detecting intruders on a campus network: might the threat be coming from within?
Rich Henders, Bill Opdyke
November 2005 **Proceedings of the 33rd annual ACM SIGUCCS conference on User services SIGUCCS '05**
Publisher: ACM Press
Full text available: pdf(188.88 KB) Additional Information: full citation, abstract, references, index terms

Campus networks, and the Information Technology organizations that support these networks, are facing security threats that are increasing in both size and complexity. Students, faculty and (non-academic) staff collectively provide a broad set of expectations and challenges to securely support. Intrusive actions and security challenges may originate outside or within a network. Security and trust can be difficult to maintain in such an environment. Intrusion detection is an important part of a c ...

Keywords: intrusion detection, snort

10 Building an e-mail virus detection system for your network
Dave Jones
December 2001 **Linux Journal**, Volume 2001 Issue 92
Publisher: Specialized Systems Consultants, Inc.
Full text available: html(22.15 KB) Additional Information: full citation, abstract, index terms

Jones gives a great example of a homegrown virus protection system.

11

Behavior-based modeling and its application to Email analysis
Salvatore J. Stolfo, Shlomo Hershkop, Chia-Wei Hu, Wei-Jen Li, Olivier Nimeskern, Ke Wang
May 2006 **ACM Transactions on Internet Technology (TOIT)**, Volume 6 Issue 2
Publisher: ACM Press
Full text available: pdf(1.25 MB) Additional Information: full citation, abstract, references, index terms

The Email Mining Toolkit (EMT) is a data mining system that computes *behavior profiles or models* of user email accounts. These models may be used for a multitude of tasks including forensic analyses and detection tasks of value to law enforcement and intelligence agencies, as well for as other typical tasks such as virus and spam detection. To demonstrate the power of the methods, we focus on the application of these models to detect the early onset of a viral propagation without "c ...

Keywords: Email virus propagations, anomaly detection, behavior profiling

12 Development and delivery of a computer security strategy for a community of end users
Allan R. Jones
December 1992 **Proceedings of the 20th annual ACM SIGUCCS conference on User services**
Publisher: ACM Press
Full text available: pdf(456.80 KB) Additional Information: full citation, index terms

13 Workshop on architectural support for security and anti-virus (WASSA): Using instruction block signatures to counter code injection attacks
Milena Milenković, Aleksandar Milenković, Emil Jovanov
March 2005 **ACM SIGARCH Computer Architecture News**, Volume 33 Issue 1
Publisher: ACM Press
Full text available: pdf(283.67 KB) Additional Information: full citation, abstract, references, index terms

With more computing platforms connected to the Internet each day, computer system security has become a critical issue. One of the major security problems is execution of malicious injected code. In this paper we propose new processor extensions that allow execution of trusted instructions only. The proposed extensions verify instruction block signatures in run-time. Signatures are generated during a trusted installation process, using a multiple input signature register (MISR), and stored in an ...

14 The costly implications of consulting in a virus-infected computer environment
K. Nunez, T. Gerace, A. Hartman
October 1989 **Proceedings of the 17th annual ACM SIGUCCS conference on User Services**
Publisher: ACM Press
Full text available: pdf(468.70 KB) Additional Information: full citation, index terms

15 WBIA'05: ASM: application security monitor
Micha Moffie, David Kaeli
December 2005 **ACM SIGARCH Computer Architecture News**, Volume 33 Issue 5
Publisher: ACM Press
Full text available: pdf(246.65 KB) Additional Information: full citation, abstract, references, index terms

Our Application Security Monitor *(ASM) is a run-time monitor that dynamically collects* *execution-related data. ASM is part of a security framework that will allow us to explore different security policies aimed at identifying malicious behavior such as Trojan horses and backdoors.In this paper, we show what type of data ASM can collect and illustrate how this data can be used to enforce a security policy. Using ASM we are able to explore different tradeoffs between security and ...*

16 Intrusion detection and response: MET: an experimental system for Malicious Email Tracking

Manasi Bhattacharyya, Shlomo Hershkop, Eleazar Eskin

September 2002 **Proceedings of the 2002 workshop on New security paradigms**

Publisher: ACM Press

Full text available: pdf(790.18 KB) Additional Information: full citation, abstract, references, citings, index terms

Despite the use of state of the art methods to protect against malicious programs, they continue to threaten and damage computer systems around the world. In this paper we present MET, the Malicious Email Tracking system, designed to automatically report statistics on the flow behavior of malicious software delivered via email attachments both at a local and global level. MET can help reduce the spread of malicious software worldwide, especially self-replicating viruses, as well as provide furth ...

Keywords: anti-virus, email attachment, email tracking, virus detection

17 Security considerations for remote electronic voting

Aviel D. Rubin

December 2002 **Communications of the ACM**, Volume 45 Issue 12

Publisher: ACM Press

Full text available: pdf(209.26 KB) html(31.18 KB) Additional Information: full citation, abstract, references, index terms

Introducing state-of-the art technology into the election process implies new risks that may not be worth taking.

18 Conscientious software

Richard P. Gabriel, Ron Goldman

October 2006 **ACM SIGPLAN Notices , Proceedings of the 21st annual ACM SIGPLAN conference on Object-oriented programming languages, systems, and applications OOPSLA '06**, Volume 41 Issue 10

Publisher: ACM Press

Full text available: pdf(1.52 MB) Additional Information: full citation, abstract, references, index terms

Software needs to grow up and become responsible for itself and its own future by participating in its own installation and customization, maintaining its own health, and adapting itself to new circumstances, new users, and new uses. To create such software will require us to change some of our underlying assumptions about how we write programs. A promising approach seems to be to separate software that does the work (allopoietic)from software that keeps the system alive (autopoietic).

Keywords: autopoiesis, continuous (re)design, emergence, feedback, repair, robustness, self-sustaining systems, self-testing, software, software complexity, stigmergy

19 Session 2: On the effectiveness of automatic patching

Milan VojnoviĆ, Ayalvadi Ganesh

November 2005 **Proceedings of the 2005 ACM workshop on Rapid malcode WORM '05**

Publisher: ACM Press
Full text available: pdf(702.79 KB) Additional Information: full citation, abstract, references, index terms

We study the effectiveness of automatic patching and quantify the speed of patch dissemination required for worm containment. We focus on random scanning as this is representative of current generation worms, though smarter strategies exist. We find that even such "dumb" worms require very fast patching. Our primary focus is on how delays due to worm detection and patch generation and dissemination affect worm spread. Motivated by scalability and trust issues, we consider a hierarchical system ...

Keywords: automatic updates, epidemic, minimum broadcast curve, patching, software updates, virus, worm

20 An experience of monitoring university network security using a commercial service and DIY monitoring
Masato Masuya, Takash Yamanoue, Shinichiro Kubota
November 2006 **Proceedings of the 34th annual ACM SIGUCCS conference on User services SIGUCCS '06**
Publisher: ACM Press
Full text available: pdf(282.98 KB) Additional Information: full citation, abstract, references, index terms

Monitoring network security of a university is one of the most important jobs for the network managers. Without the monitoring, it is hard to keep the network safe. It is common that the security policy of a university has the term which states that monitoring network security is a mandate. However it is very hard to monitor every part of a university's network by the limited number of staff and a limited amount of time and expense. In order to cope with these problems, we bought a commercial ne ...

Keywords: IDS, audit, fire wall, monitor, network, policy, security

Results 1 - 20 of 200 Result page: **1** 2 3 4 5 6 7 8 9 10 next

Terms used **virus detect time infection find out** Found **50,995** of **193,448**

Sort results by: relevance

Display results: expanded form

Save results to a Binder

Search Tips

□ Open results in a new window

Try an Advanced Search

Try this search in The ACM Guide

Results 1 - 20 of 200 Result page: **1** 2 3 4 5 6 7 8 9 10 next

Best 200 shown

Relevance scale

1 The monitoring and early detection of internet worms

Cliff C. Zou, Weibo Gong, Don Towsley, Lixin Gao

October 2005 **IEEE/ACM Transactions on Networking (TON)**, Volume 13 Issue 5

Publisher: IEEE Press

Full text available: pdf(594.79 KB) Additional Information: full citation, abstract, references, index terms

After many Internet-scale worm incidents in recent years, it is clear that a simple self-propagating worm can quickly spread across the Internet and cause severe damage to our society. Facing this great security threat, we need to build an early detection system that can detect the presence of a worm in the Internet as quickly as possible in order to give people accurate early warning information and possible reaction time for counteractions. This paper first presents an Internet worm monitoring ...

Keywords: computer network security, early detection, internet worm, network monitoring

2 A taxonomy of computer program security flaws

Carl E. Landwehr, Alan R. Bull, John P. McDermott, William S. Choi

September 1994 **ACM Computing Surveys (CSUR)**, Volume 26 Issue 3

Publisher: ACM Press

Full text available: pdf(3.81 MB) Additional Information: full citation, abstract, references, citings, index terms, review

An organized record of actual flaws can be useful to computer system designers, programmers, analysts, administrators, and users. This survey provides a taxonomy for computer program security flaws, with an Appendix that documents 50 actual security flaws. These flaws have all been described previously in the open literature, but in widely separated places. For those new to the field of computer security, they provide a good introduction to the characteristics of security flaws and how they ...

Keywords: error/defect classification, security flaw, taxonomy

3 Temporal search: detecting hidden malware timebombs with virtual machines

Jedidiah R. Crandall, Gary Wassermann, Daniela A. S. de Oliveira, Zhendong Su, S. Felix Wu, Frederic T. Chong

October 2006 **ACM SIGPLAN Notices , ACM SIGOPS Operating Systems Review , ACM**

SIGARCH Computer Architecture News , Proceedings of the 12th international conference on Architectural support for programming languages and operating systems ASPLOS-XII, Volume 41 , 40 , 34 Issue 11 , 5 , 5

Publisher: ACM Press

Full text available: pdf(271.78 KB) Additional Information: full citation, abstract, references, index terms

Worms, viruses, and other malware can be ticking bombs counting down to a specific time, when they might, for example, delete files or download new instructions from a public web server. We propose a novel virtual-machine-based analysis technique to automatically discover the *timetable* of a piece of malware, or when events will be triggered, so that other types of analysis can discern what those events are. This information can be invaluable for responding to rapid malware, and automating ...

Keywords: malware, virtual machines, worms

4 Technical correspondence: Analysis and detection of computer viruses and worms: an annotated bibliography

Prabhat K. Singh, Arun Lakhotia

February 2002 **ACM SIGPLAN Notices**, Volume 37 Issue 2

Publisher: ACM Press

Full text available: pdf(667.42 KB) Additional Information: full citation, abstract

This annotated bibliography reviews research in analyzing and detecting computer viruses and worms. This document focuses on papers that give information about techniques and systems detecting malicious code.

5 The internet worm program: an analysis

Eugene H. Spafford

January 1989 **ACM SIGCOMM Computer Communication Review**, Volume 19 Issue 1

Publisher: ACM Press

Full text available: pdf(2.45 MB) Additional Information: full citation, abstract, citings, index terms

On the evening of 2 November 1988, someone infected the Internet with a *worm* program. That program exploited flaws in utility programs in systems based on BSD-derived versions of UNIX. The flaws allowed the program to break into those machines and copy itself, thus *infecting* those systems. This program eventually spread to thousands of machines, and disrupted normal activities and Internet connectivity for many days.This report gives a detailed description of the components of the ...

6 A bit of viral protection is worth a megabyte of cure

Tim Fitzgerald

June 1995 **ACM SIGUCCS Newsletter**, Volume 25 Issue 1-2

Publisher: ACM Press

Full text available: pdf(427.33 KB) Additional Information: full citation, abstract, index terms

Even in today's world of safeguarded networks and advanced detection software, computer viruses are still running amok in some of the seedier niches of cyberspace and hiding out on unclean disks and unprotected hard drives. Speculative rumors of wide-spread epidemics have only added to the confusion as computer users all over the world wonder if their systems are at risk and if there is any way to shield themselves from these stealth operatives of electronic malfeasance.

7 Building an e-mail virus detection system for your network

Dave Jones

December 2001 **Linux Journal**, Volume 2001 Issue 92

Publisher: Specialized Systems Consultants, Inc.
Full text available: html(22.15 KB) Additional Information: full citation, abstract, index terms

Jones gives a great example of a homegrown virus protection system.

8 A study of retrospective and on-line event detection
Yiming Yang, Tom Pierce, Jaime Carbonell
August 1998 **Proceedings of the 21st annual international ACM SIGIR conference on Research and development in information retrieval**
Publisher: ACM Press
Full text available: pdf(1.05 MB) Additional Information: full citation, references, citings, index terms

9 Session 1: ACT: attachment chain tracing scheme for email virus detection and control
Jintao Xiong
October 2004 **Proceedings of the 2004 ACM workshop on Rapid malcode**
Publisher: ACM Press
Full text available: pdf(283.77 KB) Additional Information: full citation, abstract, references, index terms

Modern society is highly dependent on the smooth and safe flow of information over communication and computer networks. Computer viruses and worms pose serious threats to the society by disrupting the normal information flow and collecting or destroying information without authorization. Compared to the effectiveness and ease of spreading worms and viruses, currently adopted defense schemes are slow to react and costly to implement.

This paper proposes an automated email virus detecti ...

Keywords: contact tracing, transmission chain, worm defense

10 Risks to the public: Risks to the public
Peter G. Neumann
May 2005 **ACM SIGSOFT Software Engineering Notes**, Volume 30 Issue 3
Publisher: ACM Press
Full text available: pdf(177.87 KB) Additional Information: full citation, abstract, index terms

Edited by Peter G. Neumann (Risks Forum Moderator and Chairman of the ACM Committee on Computers and Public Policy), plus personal contributions by others, as indicated. Opinions expressed are individual rather than organizational, and all of the usual disclaimers apply. We address problems relating to software, hardware, people, and other circumstances relating to computer systems. To economize on space, we include pointers to items in the online Risks Forum: (R i j) denotes RISKS vol i number ...

11 Columns: Risks to the public in computers and related systems
Peter G. Neumann
January 2001 **ACM SIGSOFT Software Engineering Notes**, Volume 26 Issue 1
Publisher: ACM Press
Full text available: pdf(3.24 MB) Additional Information: full citation

12 Astrolabe: A robust and scalable technology for distributed system monitoring,

management, and data mining
Robbert Van Renesse, Kenneth P. Birman, Werner Vogels
May 2003 **ACM Transactions on Computer Systems (TOCS)**, Volume 21 Issue 2
Publisher: ACM Press
Full text available: pdf(341.62 KB) Additional Information: full citation, abstract, references, citings, index terms

Scalable management and self-organizational capabilities are emerging as central requirements for a generation of large-scale, highly dynamic, distributed applications. We have developed an entirely new distributed information management system called Astrolabe. Astrolabe collects large-scale system state, permitting rapid updates and providing on-the-fly attribute aggregation. This latter capability permits an application to locate a resource, and also offers a scalable way to track sys ...

Keywords: Aggregation, epidemic protocols, failure detection, gossip, membership, publish-subscribe, scalability

13 Graph mining: Laws, generators, and algorithms
Deepayan Chakrabarti, Christos Faloutsos
June 2006 **ACM Computing Surveys (CSUR)**, Volume 38 Issue 1
Publisher: ACM Press
Full text available: pdf(910.68 KB) Additional Information: full citation, abstract, references, index terms

How does the Web look? How could we tell an abnormal social network from a normal one? These and similar questions are important in many fields where the data can intuitively be cast as a graph; examples range from computer networks to sociology to biology and many more. Indeed, any *M* : *N* relation in database terminology can be represented as a graph. A lot of these questions boil down to the following: "How can we generate synthetic but realistic graphs?" To answer thi ...

Keywords: Generators, graphs, patterns, social networks

14 Traffic characterization: Characteristics of internet background radiation
Ruoming Pang, Vinod Yegneswaran, Paul Barford, Vern Paxson, Larry Peterson
October 2004 **Proceedings of the 4th ACM SIGCOMM conference on Internet measurement**
Publisher: ACM Press
Full text available: pdf(396.12 KB) Additional Information: full citation, abstract, references, index terms

Monitoring any portion of the Internet address space reveals incessant activity. This holds even when monitoring traffic sent to unused addresses, which we term "background radiation. " Background radiation reflects fundamentally nonproductive traffic, either malicious (flooding backscatter, scans for vulnerabilities, worms) or benign (misconfigurations). While the general presence of background radiation is well known to the network operator community, its nature has yet to be broadly charac ...

Keywords: honeypot, internet background radiation, network telescope

15 Frontmatter (TOC, Letters, Philosophy of computer science, Interviewers needed, Taking software requirements creation from folklore to analysis, SW components and product lines: from business to systems and technology, Software engineering survey)
September 2005 **ACM SIGSOFT Software Engineering Notes**, Volume 30 Issue 5

Publisher: ACM Press
Full text available: pdf(1.98 MB) Additional Information: full citation, index terms

16 An experience of monitoring university network security using a commercial service and DIY monitoring
Masato Masuya, Takash Yamanoue, Shinichiro Kubota
November 2006 **Proceedings of the 34th annual ACM SIGUCCS conference on User services SIGUCCS '06**
Publisher: ACM Press
Full text available: pdf(282.98 KB) Additional Information: full citation, abstract, references, index terms

Monitoring network security of a university is one of the most important jobs for the network managers. Without the monitoring, it is hard to keep the network safe. It is common that the security policy of a university has the term which states that monitoring network security is a mandate. However it is very hard to monitor every part of a university's network by the limited number of staff and a limited amount of time and expense. In order to cope with these problems, we bought a commercial ne ...

Keywords: IDS, audit, fire wall, monitor, network, policy, security

17 Risks to the public in computers and related systems
Peter G. Neumann
April 1993 **ACM SIGSOFT Software Engineering Notes**, Volume 18 Issue 2
Publisher: ACM Press
Full text available: pdf(1.60 MB) Additional Information: full citation, citings, index terms

18 Invited papers on the frontiers of software practice: Cybersecurity
Richard A. Kemmerer
May 2003 **Proceedings of the 25th International Conference on Software Engineering**
Publisher: IEEE Computer Society
Full text available: pdf(1.17 MB) Publisher Site Additional Information: full citation, abstract, references, index terms

As more business activities are being automated and an increasing number of computers are being used to store sensitive information, the need for secure computer systems becomes more apparent. This need is even more apparent as systems and applications are being distributed and accessed via an insecure network, such as the Internet. The Internet itself has become critical for governments, companies, financial institutions, and millions of everyday users. Networks of computers support a multitude ...

19 Columns: Risks to the public in computers and related systems
Peter G. Neumann
March 2002 **ACM SIGSOFT Software Engineering Notes**, Volume 27 Issue 2
Publisher: ACM Press
Full text available: pdf(1.54 MB) Additional Information: full citation

20 Intrusion detection for distributed applications
Matthew Stillerman, Carla Marceau, Maureen Stillman

July 1999 **Communications of the ACM**, Volume 42 Issue 7
Publisher: ACM Press
Full text available: pdf(210.29 KB) html(34.90 KB) Additional Information: full citation, references, citings, index terms

Results 1 - 20 of 200 Result page: **1** 2 3 4 5 6 7 8 9 10 next

IEEE Xplore® RELEASE 2.1

Home | Login | Logout | Access Information | Alerts |

Welcome United States Patent and Trademark Office

□ Search Results

BROWSE SEARCH IEEE XPLORE GUIDE

Results for "**((virus, time, infection, installation)<in>metadata)**"
Your search matched **300396** of **1443568** documents.
A maximum of **100** results are displayed, **25** to a page, sorted by **Relevance** in **Descending** order.

e-mail

» Search Options

View Session History

New Search

» Other Resources
(Available For Purchase)

Top Book Results

Rating of Electric Power Cables in Unfavorable Thermal Environment
by Anders, G. J.;
Hardcover, Edition: 1

Intelligent Image Processing
by Mann, S.;
Hardcover, Edition: 1

Time-Domain Methods for Microwave Structures
by Itoh, T.; Houshmand, B.;
Hardcover, Edition: 1

Communication and Computer Networks
by Woodward, M. E.;
Hardcover, Edition: 1

Time Frequency and Wavelets in Biomedical Signal Processing
by Akay, M.;
Hardcover, Edition: 1

View All 157 Result(s)

» Key

IEEE JNL	IEEE Journal or Magazine
IEE JNL	IEE Journal or Magazine
IEEE CNF	IEEE Conference Proceeding
IEE CNF	IEE Conference Proceeding
IEEE STD	IEEE Standard

Modify Search

((virus, time, infection, installation)<in>metadata) Search

□ Check to search only within this results set

Display Format: ● Citation ○ Citation & Abstract

view selected items **Select All** **Deselect All**

View: 1-25 | 26-5

□ 1. **On the time complexity of computer viruses**
Zhi-hong Zuo; Qing-xin Zhu; Ming-tian Zhou;
Information Theory, IEEE Transactions on
Volume 51, Issue 8, Aug. 2005 Page(s):2962 - 2966
Digital Object Identifier 10.1109/TIT.2005.851780
AbstractPlus | Full Text: PDF(216 KB) **IEEE JNL**
Rights and Permissions

□ 2. **Dielectric investigations of the membrane properties of baby hamster kid following infection with Herpes Simplex Virus, type 1**
Archer, S.; Rixon, F.J.; Morgan, H.;
Engineering in Medicine and Biology Society, 1998. Proceedings of the 20th A International Conference of the IEEE
Volume 6, 29 Oct.-1 Nov. 1998 Page(s):2812 - 2815 vol.6
Digital Object Identifier 10.1109/IEMBS.1998.746068
AbstractPlus | Full Text: PDF(368 KB) **IEEE CNF**
Rights and Permissions

□ 3. **New viruses up the stakes on old tricks**
Schreiner, K.;
Internet Computing, IEEE
Volume 6, Issue 4, July-Aug. 2002 Page(s):9 - 10
Digital Object Identifier 10.1109/MIC.2002.1020318
AbstractPlus | Full Text: PDF(304 KB) **IEEE JNL**
Rights and Permissions

□ 4. **Risk Assessment of Enteric Virus Disease Transmission by Shellfish Cor**
Gerba, C.; Goyal, S.;
OCEANS
Volume 19, Sep 1987 Page(s):1757 - 1760
AbstractPlus | Full Text: PDF(352 KB) **IEEE CNF**
Rights and Permissions

□ 5. **Vaccination with half dose of anti hepatitis B vaccine in Tomsk among th**
Chuikova, K.I.; Pomytkina, M.I.; Vozhakov, S.V.; Shkuratova, O.V.; Stavitskaya L.I.;
Science and Technology, 2004. KORUS 2004. Proceedings. The 8th Russian-International Symposium on

Volume 3, 26 June-3 July 2004 Page(s):331 vol. 3
Digital Object Identifier 10.1109/KORUS.2004.1555775

AbstractPlus | Full Text: PDF(220 KB) **IEEE CNF**
Rights and Permissions

□ 6. **Control of immune response of HIV infection model by gradual reduction**
Chang, H.J.; Shim, H.; Seo, J.H.;
Decision and Control, 2004. CDC. 43rd IEEE Conference on
Volume 1, 14-17 Dec. 2004 Page(s):1048 - 1054 Vol.1

AbstractPlus | Full Text: PDF(1896 KB) **IEEE CNF**
Rights and Permissions

□ 7. **The Power of the Defender**
Gelastou, M.; Mavronicolas, M.; Papadopoulou, V.; Philippou, A.; Spirakis, P.;
Distributed Computing Systems Workshops, 2006. ICDCS Workshops 2006. 2
International Conference on
04-07 July 2006 Page(s):37 - 37
Digital Object Identifier 10.1109/ICDCSW.2006.107

AbstractPlus | Full Text: PDF(264 KB) **IEEE CNF**
Rights and Permissions

□ 8. **Nonlinear control of a dynamic model of HIV-1**
Ge, S.S.; Zhiling Tian; Tong Heng Lee;
Biomedical Engineering, IEEE Transactions on
Volume 52, Issue 3, Mar 2005 Page(s):353 - 361
Digital Object Identifier 10.1109/TBME.2004.840463

AbstractPlus | Full Text: PDF(432 KB) **IEEE JNL**
Rights and Permissions

□ 9. **Analysis of HIV proteins using DSP techniques**
Cosic, I.;
Engineering in Medicine and Biology Society, 2001. Proceedings of the 23rd A
International Conference of the IEEE
Volume 3, 25-28 Oct. 2001 Page(s):2886 - 2889 vol.3

AbstractPlus | Full Text: PDF(518 KB) **IEEE CNF**
Rights and Permissions

□ 10. **Electrostatic treatment of bean seeds**
Morar, R.; Munteanu, R.; Simion, E.; Munteanu, I.; Dascalescu, L.;
Industry Applications Conference, 1995. Thirtieth IAS Annual Meeting, IAS '95
Record of the 1995 IEEE
Volume 2, 8-12 Oct. 1995 Page(s):1335 - 1337 vol.2
Digital Object Identifier 10.1109/IAS.1995.530456

AbstractPlus | Full Text: PDF(344 KB) **IEEE CNF**
Rights and Permissions

□ 11. **Towards a testbed for malicious code detection**
Lo, R.; Kerchen, P.; Crawford, R.; Ho, W.; Crossley, J.; Fink, G.; Levitt, K.; Ols
M.;
Compcon Spring '91. Digest of Papers
25 Feb.-1 March 1991 Page(s):160 - 166
Digital Object Identifier 10.1109/CMPCON.1991.128800

AbstractPlus | Full Text: PDF(472 KB) **IEEE CNF**
Rights and Permissions

□ 12. **Internet quarantine: requirements for containing self-propagating code**
Moore, D.; Shannon, C.; Voelker, G.M.; Savage, S.;
INFOCOM 2003. Twenty-Second Annual Joint Conference of the IEEE Compı
Communications Societies. IEEE

Volume 3, 30 March-3 April 2003 Page(s):1901 - 1910 vol.3
AbstractPlus | Full Text: PDF(302 KB) **IEEE CNF**
Rights and Permissions

□ 13. **On computer viral infection and the effect of immunization**
Chenxi Wang; Knight, J.C.; Elder, M.C.;
Computer Security Applications, 2000. ACSAC '00. 16th Annual Conference
11-15 Dec. 2000 Page(s):246 - 256
Digital Object Identifier 10.1109/ACSAC.2000.898879
AbstractPlus | Full Text: PDF(1496 KB) **IEEE CNF**
Rights and Permissions

□ 14. **The role of virus infection in virus-evolutionary genetic algorithm**
Kubota, N.; Shimojima, K.; Fukuda, T.;
Evolutionary Computation, 1996., Proceedings of IEEE International Conferen
20-22 May 1996 Page(s):182 - 187
Digital Object Identifier 10.1109/ICEC.1996.542357
AbstractPlus | Full Text: PDF(504 KB) **IEEE CNF**
Rights and Permissions

□ 15. **The impact of countermeasure propagation on the prevalence of comput**
Li-Chiou Chen; Carley, K.M.;
Systems, Man and Cybernetics, Part B, IEEE Transactions on
Volume 34, Issue 2, April 2004 Page(s):823 - 833
Digital Object Identifier 10.1109/TSMCB.2003.817098
AbstractPlus | References | Full Text: PDF(592 KB) **IEEE JNL**
Rights and Permissions

□ 16. **Spaceflight conditions alter human immunity and predispose to infection**
Shearer, W.T.; Butel, J.S.; Reuben, J.M.; Gridey, D.S.; White, R.J.; Gerzer, R.
[Engineering in Medicine and Biology, 2002. 24th Annual Conference and the
Meeting of the Biomedical Engineering Society] EMBS/BMES Conference, 20(
of the Second Joint
Volume 3, 23-26 Oct. 2002 Page(s):2155 - 2156 vol.3
AbstractPlus | Full Text: PDF(336 KB) **IEEE CNF**
Rights and Permissions

□ 17. **The Virus Encyclopedia: reaching a new level of information comfort**
Ashmanov, I.; Kasperskaya, N.;
Multimedia, IEEE
Volume 6, Issue 3, July-Sept. 1999 Page(s):81 - 84
Digital Object Identifier 10.1109/93.790614
AbstractPlus | Full Text: PDF(508 KB) **IEEE JNL**
Rights and Permissions

□ 18. **Compact installation for radiation processing of materials by accelerated**
Krylov, S.; Latypov, T.; Mamaev, G.; Mamaev, S.; Microchnik, E.; Priozhenko,
S.; Seleznev, I.; Tenjakov, I.; Korolev, A.; Simonov, K.;
Particle Accelerator Conference, 1999. Proceedings of the 1999
Volume 4, 27 March-2 April 1999 Page(s):2567 - 2569 vol.4
Digital Object Identifier 10.1109/PAC.1999.792778
AbstractPlus | Full Text: PDF(236 KB) **IEEE CNF**
Rights and Permissions

□ 19. **Artificial intelligence techniques for monitoring dangerous infections**
Lamma, E.; Mello, P.; Nanetti, A.; Riguzzi, F.; Storari, S.; Valastro, G.;
Information Technology in Biomedicine, IEEE Transactions on
Volume 10, Issue 1, Jan. 2006 Page(s):143 - 155
Digital Object Identifier 10.1109/TITB.2005.855537

AbstractPlus | Full Text: PDF(288 KB) **IEEE JNL**
Rights and Permissions

□ **20. Schema representation in virus-evolutionary genetic algorithm for knaps**
Kubota, N.; Fukuda, T.;
Evolutionary Computation Proceedings, 1998. IEEE World Congress on Comp
Intelligence., The 1998 IEEE International Conference on
4-9 May 1998 Page(s):834 - 839
Digital Object Identifier 10.1109/ICEC.1998.700160

AbstractPlus | Full Text: PDF(492 KB) **IEEE CNF**
Rights and Permissions

□ **21. A Bayesian approach to virus-gene expression time course data**
I-Shou Chang; Chi-Chung Wen; Yuh-Jenn Wu; Gupta, P.K.; Shih Sheng Jiang
Hsiung, C.A.;
Emerging Information Technology Conference, 2005.
15-16 Aug. 2005 Page(s):2 pp.
Digital Object Identifier 10.1109/EITC.2005.1544357

AbstractPlus | Full Text: PDF(87 KB) **IEEE CNF**
Rights and Permissions

□ **22. Some properties of timed token medium access protocols**
Valenzano, A.; Montuschi, P.; Ciminiera, L.;
Software Engineering, IEEE Transactions on
Volume 16, Issue 8, Aug. 1990 Page(s):858 - 869
Digital Object Identifier 10.1109/32.57628

AbstractPlus | Full Text: PDF(1004 KB) **IEEE JNL**
Rights and Permissions

□ **23. The effect of computer virus occurrence and virus threat level on antivirı financial performance**
Harrald, J.R.; Schmitt, S.A.; Shrestha, S.;
Engineering Management Conference, 2004. Proceedings. 2004 IEEE Interna
Volume 2, 18-21 Oct. 2004 Page(s):780 - 784 Vol.2
Digital Object Identifier 10.1109/IEMC.2004.1407486

AbstractPlus | Full Text: PDF(590 KB) **IEEE CNF**
Rights and Permissions

□ **24. Replacement kit for cement mill gearboxes**
Chetelat, D.;
Cement Industry Technical Conference, 2000 IEEE-IAS/PCA
7-12 May 2000 Page(s):69 - 78
Digital Object Identifier 10.1109/CITCON.2000.848511

AbstractPlus | Full Text: PDF(1032 KB) **IEEE CNF**
Rights and Permissions

□ **25. Influence of high-frequency electrotechnological installations on generat harmonics in a network**
Blinov, Y.; Kachanov, B.; Ishin, V.;
Electronic Instrument Engineering Proceedings, 2000. APEIE-2000. Volume 1
International Conference on Actual Problems of
26-29 Sept. 2000 Page(s):50 - 53
Digital Object Identifier 10.1109/APEIE.2000.913087

AbstractPlus | Full Text: PDF(272 KB) **IEEE CNF**
Rights and Permissions

View: 1-25 | 26-5

Help Contact Us Privacy & :

Indexed by Inspec®